IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

DYLAN MORRIS, individually and on behalf of all others similarly situated, Plaintiff, v. GATEWAY REHABILITATION CENTER, d/b/a GATEWAY REHAB, Defendant.	Case No. 2:22-cv-1678 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Dylan Morris ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendant Gateway Rehabilitation Center d/b/a Gateway Rehab ("Gateway" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE CASE

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending

risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. As a healthcare provider, specifically a provider of drug and alcohol treatment, Defendant knowingly obtains sensitive patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

4. Defendant's Notice of Privacy Practices states: "The confidentiality of alcohol and drug abuse patient records is specifically protected by state and federal laws."[1] The Notice of Privacy Practices further informs patients how Gateway "may use and share [patients'] protected health information ("PHI") as well as [patients'] rights regarding [their] PHI."[2]

5. Plaintiff brings this class action on behalf of individual patients whose PII and/or PHI was accessed and exposed to unauthorized third parties during a data breach of Defendant's system, which Defendant discovered on June 13, 2022, but did not disclose until November 18, 2022 (the "Data Breach").[3]

6. For the duration of the Data Breach, the unauthorized third parties had unrestricted access to PII and PHI in Gateway's systems.

7. Despite that Gateway became aware of the Data Breach on June 13, 2022, it failed to notify Plaintiff and the putative Class Members within 60 days as required by law. Notably,

---

[1] *Notice of Privacy Practices*, Gateway Rehabilitation Center (Oct. 28, 2021), https://www.gatewayrehab.org/resources/about/policies.
[2] *Id.*
[3] *Notice of Data Secuirty Event* (Nov. 18, 2022), https://storage.googleapis.com/treatspace-prod-media/pracf/u-2548/Gateway_Rehab_-_Substitute_Notice_-_For_Web_Only.pdf.

Defendant failed to notify Plaintiff and putative Class Members for approximately five months from its discovery of the Data Breach.

8. Plaintiff, on behalf of himself and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of fiduciary duty, breach of confidences, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

9. Based on the public statements of Defendant to date, a wide variety of PII and PHI was implicated in the breach, including but not limited to name, date of birth, Social Security Numbers, driver's license and state ID numbers, financial account and payment card information, medical information, and health insurance information.[4]

10. As a direct and proximate result of Defendant's inadequate data security, and its breach of its duty to handle PII and PHI with reasonable care, Plaintiff's and Class Members' PII and PHI has been accessed by hackers, posted on the dark web, and exposed to an untold number of unauthorized individuals.

11. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

12. To recover from Defendant for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and

[4] *Id.*

PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

13. Plaintiff Dylan Morris is an adult who at all relevant times is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff was a patient of Defendant.

14. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII—time which he would not have had to expend but for the Data Breach.

15. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

16. Defendant Gateway Rehabilitation Center is a non-profit incorporated in the Commonwealth of Pennsylvania with a principal place of business located at 100 Moffett Run Road, Aliquippa, Pennsylvania 15001. Defendant Gateway operates under the fictitious name, Gateway Rehab.

17. Defendant Gateway offers outpatient, inpatient, and extended drug and alcohol addiction treatment care at thirteen locations throughout Western Pennsylvania and Eastern Ohio.[5]

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of

[5] *See GatewayRehab*, https://www.gatewayrehab.org/ (last visited Nov. 28, 2022).

the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

19. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

20. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

FACTUAL BACKGROUND

A. Gateway and the Services it Provides.

21. Gateway is the largest drug rehab and addition recovery network in the greater Pittsburgh region, offering patients long-term treatment for drug and alcohol addiction through services focused on clinical practice, recovery support, education, and research.[6]

22. While administering these services and treatment, Defendant receives, creates, and handles PII and PHI, which includes, *inter alia*, patients' full name, address, date of birth, Social Security Number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

23. Patients must entrust their PII and PHI to Defendant to receive care, and in return, they reasonably expect that Defendant will safeguard their highly sensitive information and keep their PHI confidential.

[6] *Id.*; *Our Vision*, GatewayRehab, https://www.gatewayrehab.org/resources/about/vision-values (last visited Nov. 28, 2022).

24. Even though Gateway "takes the security and privacy of patient information very seriously"[7] Gateway nevertheless employed inadequate data security measures to protect and secure the PII and PHI patients entrusted to it, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII and PHI.

B. Defendant Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to its Patients.

25. At all relevant times, Defendant knew it was storing sensitive PII and PHI and that, as a result, its systems would be attractive for cybercriminals.

26. Defendant also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

27. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

28. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as well as the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[8] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

29. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses,

[7] *Notice of Data Secuirty Event*, *supra* note 3.
[8] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[9]

30. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[10]

31. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[11]

32. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[12]

33. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

34. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even

---

[9] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[10] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Nov. 28, 2022).

[11] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Nov. 28, 2022).

[12] *Id.*

seen $60 or $70."[13] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[14]

35. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[15]

36. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that

---

[13] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[14] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Nov. 23, 2022).

[15] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[16]

37. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

38. Based on the value of its patients' PII and PHI to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Defendant Breached its Duty to Protect its Patients' PII and PHI.

39. On June 13, 2022, Defendant announced that it experienced a security incident disrupting access to its systems.[17]

40. According to Gateway, it engaged forensics and incident response experts to investigate the Data Breach.[18] By July 8, 2022, the investigation confirmed that data containing PII and PHI may have been accessed or acquired by an unauthorized third party.[19]

41. After the investigation revealed that PII and PHI may have been accessed or acquired by an unauthorized third party, Gateway then conducted a review process to confirm what

[16] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Nov. 28, 2022).
[17] *Notice of Data Secuirty Event*, *supra* note 3.
[18] *Id.*
[19] *Id.*

it already knew—that PII and PHI of current and former patients had been compromised.[20] This review process took an additional two months and was completed on September 21, 2022.[21]

42. The patient PII and PHI compromised in the Data Breach includes patient names, dates of birth, Social Security Numbers, driver's license or state ID numbers, financial account and/or payment information, medical information, and health insurance information.[22]

43. While Gateway asserts that it "has no evidence that any of this information was misused,"[23] on or around July 8, 2022, DataBreaches.net reported that Gateway was the apparent victim of a ransomware attack by the hacker group BlackByte.[24] BlackByte leaked Gateway files containing PII and PHI on its ransomware website located on the dark web.[25]

44. Blackbyte leaked more than 4 GB of Gateway's data onto the dark web.[26] The leaked data contained numerous documents, including documents that include sensitive and personal information on patients, such as their arrest records and history of behavior and substance related issues.[27]

---

[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *A Community Health Provider in Vermont and an Addiction Rehab Organization in Pennsylvania Fall Prey to BlackByte*, DataBreaches (July 8, 2022), https://www.databreaches.net/a-community-health-provider-in-vermont-and-an-addiction-rehab-organization-in-pennsylvania-fall-prey-to-blackbyte/.
[25] *Id.*
[26] *Id.*
[27] *Id.*

45. Despite BlackByte leaking Gateway's patient PII and PHI on its ransomware site on or around July 8, 2022, Gateway did not report the Data Breach to the Department of Health and Human Services Office for Civil Rights ("HHS") until November 18, 2022.[28]

46. On or about the same date that Gateway reported the Data Breach to HHS, Gateway provided notice to Plaintiff indicating that his/her PII and PHI may have been compromised or accessed during the Data Breach, approximately five months after Gateway first discovered the Data Breach.

47. Like Plaintiff, the Class Members received similar notices informing them that their PII and/or PHI was exposed in the Data Breach.

48. All in all, more than 130,000 patients of Gateway had their PII and/or PHI breached.[29]

49. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect its patients' PII and PHI.

50. BlackByte is a ransomware group that debuted in July 2021.[30] BlackByte quickly gained a name for itself and was identified by the Federal Bureau of Investigation and the United Sates Secret Service as a new, noteworthy ransomware variant.[31]

---

[28] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 28, 2022).
[29] *Id.*
[30] *Ransomware Spotlight BlackByte*, Trend Micro (July 5, 2022), https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte.
[31] *Id.*

51. "BlackByte is a Ransomware as a Service (RaaS) group that encrypts files on compromised Windows host systems, including physical and virtual servers."[32] "BlackByte has been known to use phishing emails or exploit unpatched PorxyShell vulnerability in Microsoft Exchange Servers to gain initial access into a system."[33]

52. "As of December 8th, 2021, Blackbyte uses the anonymous file upload sites of 'anonymfiles[.]com' and 'file[.]io.' It is recommended to block these sites on your firewall/proxy technologies in order to reduce the likelihood of data exfiltration."[34]

53. Upon information and belief, Defendant failed to implement one or more of the following data security measures to mitigate the risk of a ransomware attack, regardless of any variant, including BlackByte:

> Regularly monitor and audit external facing services and assets for accidental exposure and out-of-date services. Remove any accidental exposure and patch any out-of-date services, with priority on services that have known vulnerabilities. Threat Actors will frequently scan the internet for public-facing assets that have an exploitable vulnerability and gain initial access via this method.
>
> Implement phishing training and deploy e-mail security technologies to mitigate the risk of malicious e-mail documents. Threat actor groups often conduct phishing campaigns with malicious documents in order to gain an initial foothold.
>
> Ensure comprehensive coverage of Anti-Virus/Endpoint Detection and Response tools within your environment in order to provide as much visibility as possible into exploit/threat activity.
>
> Maintain regular backups of all critical systems/information. Maintain offline backups as well to increase resilience.

---

[32] Sergiu Gatlan, *FBI: BlackByte Ransomware Breached US Critical Infrastructure*, BleepingComputer (Feb. 14, 2022), https://www.bleepingcomputer.com/news/security/fbi-blackbyte-ransomware-breached-us-critical-infrastructure/.
[33] Trend Micro, *supra* note 30.
[34] *Threat Advisory: Blackbyte Ransomware*, ReliaQuest, https://www.reliaquest.com/blog/threat-advisory-blackbyte-ransomware/ (last updated Feb. 13, 2022).

> Enforce complex passwords and Multi-Factor Authentication across all aspects of the environment (including third-party accounts).[35]

D. Plaintiff and Class Members Suffered Damages.

54. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused the Plaintiff and members of the Class significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

55. Once PII and PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

56. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PHI.

57. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those

[35] *Id.*

affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[36]

58. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[37]

59. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[38]

60. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[39]

61. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[40] This is especially true where here, the medical information at issue involves patients' drug and alcohol abuse treatments and this information has already been leaked on the dark web.

---

[36] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Nov. 28, 2022).
[37] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HealthITSecurity, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited Nov. 28, 2022).
[38] *Id.*
[39] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[40] *Id.*

62. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[41]

63. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

64. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

65. Plaintiff brings this class action on behalf of himself and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

66. Plaintiff seeks to represent a class of persons to be defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised in the Gateway Data Breach which was announced on or about November 18, 2022 (the "Class").

67. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

---

[41] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, Experian, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Nov. 28, 2022).

68. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

69. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 130,000 individuals.

70. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Defendant breached its fiduciary duty to Plaintiff and the Class;

d. Whether Defendant breach its duty of confidence to Plaintiff and the Class;

e. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

f. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

71. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise

from the same unlawful and willful conduct. Plaintiff and members of the Class were all patients of Defendant, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

72. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

73. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

74. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

75. **Injunctive Relief –** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

76. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

77. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

78. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

79. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

80. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

81. Defendant's duty also arose from Defendant's position as a healthcare provider. Defendant holds itself out as a trusted provider of healthcare, and thereby assumes a duty to

reasonably protect its patients' information. Indeed, Defendant who directly provides comprehensive addiction treatment, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

82. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiff's and Class Members' PII and PHI, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

83. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

84. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

85. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

86. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

87. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

88. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving PII and PHI of its patients.

89. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

90. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

91. Defendant is an entity covered under HIPAA which sets minimum federal standards for privacy and security of PHI.

92. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendant had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class Members' electronic PHI.

93. Specifically, HIPAA required Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et. seq*.

94. Defendant violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

95. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect.

96. Defendant's violation of HIPAA constitutes negligence *per se*.

97. Defendant is a substance abuse disorder treatment provider covered under the Confidentiality of Alcohol and Drug Abuse Patient Records Act and its implementing regulations, 42 U.S.C. § 290dd-2; 42 CFR Part 2 (collectively "Part 2"), which set limits on the use and disclosure of a substance abuse disorder patient's records.

98. Under Part 2, Defendant was required to maintain the confidentiality of substance abuse disorder treatments and was prohibited from disclosing information in a substance abuse disorder patient's medical record, unless Defendant obtained consent or identified an exception that specifically authorized the disclosure.

99. Plaintiff's and Class Members' medical records are substance abuse disorder medical records covered by Part 2.

100. Plaintiff and Class Members did not consent to the disclosure of their confidential substance abuse medical records by Defendant nor was Defendant authorized to disclose Plaintiff's and Class Members' confidential substance abuse medical records to unknown cyber criminals.

101. Defendant violated Part 2 by actively disclosing Plaintiff's and the Class Members' electronic PHI to unknown cyber criminals.

102. Plaintiff and the Class Members are patients within the class of persons Part 2 was intended to protect.

103. Defendant's violation of Part 2 constitutes negligence *per se*.

104. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act, HIPAA, and Part 2 was intended to guard against.

105. As a direct and proximate result of Defendant's negligence, Plaintiff's and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

106. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

107. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

108. As a healthcare provider, and recipient of patients' PII and PHI, Defendant has a fiduciary relationship to its patients, like Plaintiff and the Class Members.

109. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable PHI and PII related to Plaintiff and the Class. Plaintiff and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

110. Defendant owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

111. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiff's and the Class Members' medical records.

112. Defendant's patients, like Plaintiff and Class Members, have a privacy interest in personal medical matters, and Gateway had a fiduciary duty not to disclose medical data concerning its patients.

113. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII and PHI of Plaintiff and Class Members, information not generally known.

114. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their PII and PHI to unknown criminal actors.

115. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to

adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

116. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

117. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

118. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

119. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

120. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

121. As a healthcare provider, Defendant has a special relationship to its patients, like Plaintiff and the Class Members.

122. Because of that special relationship, Defendant was provided with and stored private and valuable PHI related to Plaintiff and the Class, which it was required to maintain in confidence.

123. Plaintiff and the Class provided Defendant with their personal and confidential PHI under both the express and/or implied agreement of Defendant to limit the use and disclosure of such PHI.

124. Defendant owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

125. Defendant had an obligation to maintain the confidentiality of Plaintiff's and the Class members' PHI.

126. Plaintiff and Class Members have a privacy interest in their personal medical matters, and Defendant had a duty not to disclose confidential medical information and records concerning its patients.

127. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PHI and confidential medical records of Plaintiff and Class Members.

128. Plaintiff's and the Class's PHI is not generally known to the public and is confidential by nature.

129. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their PHI to an unknown criminal actor.

130. Defendant breached the duties of confidence it owed to Plaintiff and Class Members when Plaintiff's and the Class's PHI was disclosed to unknown criminal hackers.

131. Defendant breached its duties of confidence by failing to safeguard Plaintiff's and Class Members' PHI, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; (h) storing PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class Members' PHI and medical records/information to a criminal third party.

132. But for Defendant's wrongful breach of its duty of confidences owed to Plaintiff and Class Members, their privacy, confidences, and PHI would not have been compromised.

133. As a direct and proximate result of Defendant's breach of Plaintiff's and the Class's confidences, Plaintiff and Class Members have suffered injuries, including:

a. The erosion of the essential and confidential relationship between Defendant – as a health care services provider – and Plaintiff and Class Members as patients;

b. Loss of their privacy and confidentiality in their PHI;

c. Theft of their PII and/or PHI;

d. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

e. Costs associated with purchasing credit monitoring and identity theft protection services;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Gateway Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

i. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

j. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendant; and

l. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PHI.

134. Additionally, Defendant received payments from Plaintiff and Class Members for services with the understanding that Defendant would uphold its responsibilities to maintain the confidences of Plaintiff's and Class Members' private medical information.

135. Defendant breached the confidence of Plaintiff and Class Members when it made an unauthorized release and disclosure of their confidential medical information and/or PHI and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiff's and Class Members' expense.

136. As a direct and proximate result of Defendant's breach of its duty of confidences, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

137. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

138. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

139. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and PHI and remains at imminent risk that further compromises of his PII and/or PHI will occur in the future.

140. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed a legal duty to secure patients' PII and PHI under the common law, Section 5 of the FTC Act, HIPAA, and Part 2; and

b. Defendant breached and continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

141. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

142. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Gateway. The risk of another such breach is real, immediate, and substantial. If another breach at Gateway occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

143. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant have a pre-existing legal obligation to employ such measures.

144. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Gateway, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: November 28, 2022

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch
Jamisen A. Etzel
Nicholas A. Colella
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
P: (412) 322-9243
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com

Attorneys for Plaintiff